Password Policy Discovery, Technique T1201 - Enterprise

Archived: 2026-04-05 15:31:49 UTC

Adversaries may attempt to access detailed information about the password policy used within an enterprise network or cloud environment. Password policies are a way to enforce complex passwords that are difficult to guess or crack through Brute Force. This information may help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks which adheres to the policy (e.g. if the minimum password length should be 8, then not trying passwords such as 'pass123'; not checking for more than 3-4 passwords per account if the lockout is set to 6 as to not lock out accounts).

Password policies can be set and discovered on Windows, Linux, and macOS systems via various command shell utilities such as `net accounts (/domain)`, `Get-ADDefaultDomainPasswordPolicy`, `chage -l`, `cat /etc/pam.d/common-password`, and `pwpolicy getaccountpolicies` [1] [2]. Adversaries may also leverage a Network Device CLI on network devices to discover password policy information (e.g. `show aaa`, `show aaa common-criteria policy all`).[3]

Password policies can be discovered in cloud environments using available APIs such as `GetAccountPasswordPolicy` in AWS [4].

Source: https://attack.mitre.org/techniques/T1201